General

In response to the introduction of the General Data Protection Regulation 2018, Card Geotechnics Limited (CGL) has formulated the following policy and identified the key elements with regard to compliance with the Regulation, which came into force on 25 May 2018.

Information held

CGL as an organisation providing professional consultancy services into the construction industry holds the following types of information. These are held electronically on servers within CGL offices and protected from hacking and unauthorised access by firewall and installed malware protection software, regularly updated by CIT, CGL's specialist company IT support contractor. Activities are monitored 24/7 by CIT in order to protect CGL's data from disruption and unauthorised usage of data held.

Employed staff: As a UK employer CGL holds the personal data of staff relevant to the requirements of employment in the business. This data includes, full names, addresses and identified next of kin, phone numbers (mobile and landlines as relevant) and records of driving licences and passports supplied by an individual during the induction process at commencement of employment or during the normal upgrading of data for the commercial activity of the company. For employee remuneration and pension purposes, financial information supplied by the individual member of staff is held by CGL. All such data on current staff is held in electronic files with access restricted by the IT software permissions to senior staff with Finance/Human Resource functions, and the Directors and Regional Directors. This data is not shared with those outside these functions.

Former staff: Details limited to information supplied by the employee at the time of their employment or generated during their employment with CGL are held in separate password protected archived electronic files. Such files are subject to an annual review with the purpose of limiting the held information on any specific ex member of staff to record employment period, grade, location of employment and reason for leaving CGL.

Client information: Within PIMS (the CGL practice management system) CGL holds the contact details of client and supplier information with information on personnel of relevance to the normal day to day commercial activities of the company in providing specialist consultancy advice to the construction industry. This information has been supplied by the individual and companies for the purposes of undertaking commercial activity, business to business, with CGL. This data set was audited for relevance and currency in November/December 2017 for incorporation into PIMS. This data set is under continual review for relevance. CGL limits collection and retaining of data to publicly available addresses and contact details (usually from the companies' own web sites) provided to its own staff during the course of their normal professional duties.

Marketing data: Such data as is collected for marketing of professional services to prospective clients by CGL is taken from publicly available information on company web sites and the use of social media sources; predominantly LinkedIn. Such data is limited and commonly in the form of business email addresses, web site contact details and published work addresses. Data entered on to the CRM portion of PIMS was audited in November/December 2017 and is regularly reviewed for validity. Expired or unwanted addresses are deleted from records.

Requests for information

Staff requesting data information held on them by CGL will be provided the information in accordance with the appropriate UK regulations. These would include but not be limited to: such

information provided by them during the recruitment and induction programmes, appraisal documentation, copies of any formal disciplinary documentation and promotion and remuneration correspondence. Such information will not be provided to any other organisation or individual without the express permission of the staff member whose data it is.

Requests from external parties or individuals will be provided with the data held by CGL on receipt of a third party verified, written request from that individual or organisation. Responses will be provided within one calendar month.

Requests will not normally be refused. However, CGL reserves the right to refuse an access request but will provide reasons if it is decided to do so. An applicant will have the right to raise a complaint with the Information Commissions Office ICO or their agent in these matters.

Reasons for processing held data

The three types of data set are processed in different ways and according to the *Legitimate Interest** of CGL and the business needs of a specialist geotechnical and geoenvironmental engineering consultancy.

Defined legitimate interest

1. Direct marketing

The GDPR states, 'the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.'

This may be where consent is not viable or not preferred, though the DPN rightly stresses the fact that organisations will still need to show that there is a balance of interests – their own and those of the person receiving the marketing.

Of course, any individual can object to direct marketing and it is one of the examples of legitimate interests for which objection is already fairly well understood and easy to action (often by unsubscribe link or by contacting the company in question to request).

2. Relevant and appropriate relationship

This may be a direct appropriate relationship, such as where the individual is a client.

3. Reasonable expectations

As previously discussed, if a controller understands individuals have a reasonable expectation their data will be processed, this may help to make a case for legitimate interests.

Employed staff: CGL holds such data to facilitate staff remuneration, reward and employment responsibilities. Process of the data is limited to undertaking these activities in as efficient and equitable manner as possible.

Former staff: The data will not be processed save as to present either by name or employment date to facilitate reference requirements from other employers or organisations recognised as having a reasonable need to request such data.

Client information: Client data will be processed within the CGL practice management software system (PIMS) to facilitate communication, professional advice and subcontracting of work for the normal day to day activities of CGL as a professional practice consultancy. Such data can be accessed via desk PCs and portable devices, such as laptops, tablets and telephones. These devices have password access to allow data to be read. Such information is of non-personal nature and found in the public domain placed there by the individual or firm involved. It is not CGL's practice to buy commercial listing of client prospects and this continues to remain policy.

CGL will continue to have an interest in making sure the marketing relevant to clients, and CGL will only process information so as to focus any marketing to the interests of the business organisation and the individual within it. When doing this, CGL will process any personal information only for *legitimate interest** and will consider and balance any potential impact on an individual (both positive and negative), and their rights under data protection laws.

It is recognised that CGL *legitimate interests* do not automatically override the interests of an individual and the company will not use personal data for activities where company interests are overridden by the impact on the individual unless CGL has an individual's consent or are otherwise required or permitted to by law.

Impact on children and minors

During the course of its *legitimate interest* business activities concerned with engineering consultancy, CGL will not be collecting any data relating to children and minors or, on balance of probabilities, risk receiving data from such individuals.

From time to time information on minors and dependants of employees may be provided for the purpose of processing health benefits to senior staff. Such information would form part of confidential information provided to third party health insurance providers only and would not normally be retained within the personal files of employees. Any listing would be located in secure personnel files accessed only through direct authorisation for senior staff and only for the strict purpose of providing benefits to employees.

IT Security and restriction of access to data bases of information

The Personnel HR Directory is restricted by using the Personnel Security Group, only Domain Administrators have access to add and remove users from this group. All documents are restricted to CGL staff that have domain users accounts.

The practice management software, PIMS, requires a separate user account for access. Groups are used to restrict access to specific areas of PIMS.

Godalming, Harrogate and Exeter are protected 24/7 by a Cloud hosted Watchguard XTMV provided by Elite Telecom. The London office which is a serviced office and has a Watchguard XTM 26 installed to protect and allow connectivity into the MPLS.

Servers have Windows Updates installed at least quarterly and are monitored for unauthorised attempts using RMC (Remote Management Console), user accounts are set to lock out after 5 invalid attempts. A check is in place for unauthorised access attempts that is recorded in RMC.

All PCs have Webroot (Antivirus) and Web Protection installed. PCs are scanned daily and servers weekly for viruses. All emails are filtered through Cloud Mail Security (Spam Filter)

All servers are backed up to an onsite device (Datto SIRIS 10000) and are then replicated offsite, all onsite backups are encrypted. A check is put in place for signs of Ransomware and an email alert is sent out to the London Helpdesk, onsite person and Technical Consultant.

All archived data are stored on a separate server that has restricted access, which is given by the Domain Administrator (CIT).

CGL has a password policy to ensure the security of user accounts. All people that have access to CGL systems are required to use Multi Factor Authentication (MFA).

CGL complies with the requirements of the Cyber Essentials Scheme; registration number: QGCE 3124.

Data protection impact assessments

Where new IT infrastructure is proposed, or profiling departs from the expressed methodologies designed to focus materials to client company needs or new data sets of a significantly different nature to those already collected, a Data Protection Impact Assessment (DPIA) will be undertaken and the results reported to the Board of CGL at the next scheduled meeting, or a specially convened meeting if deemed necessary by the CGL Data Protection Officer (see below).

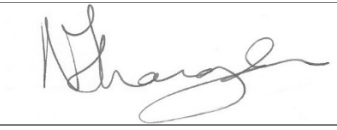
A risk review of data breach, system penetration and hacking of company information will form part of the regular quarterly Risk Review reported at each Board.

Data Protection Officer

The Data Protection Officer is currently Nick Langdon, Business Director who will act in the final role as Controller on matters of data policy.

International

CGL currently has a presence in Dublin, with an individuals providing support to UK operations. As the office is currently configured there are no plans for local cached server operations and access to IT systems is through password protected individual access for remote access working. Data of a sensitive nature will not be left on any local PC/laptop but will be retained within the single CGL UK based IT framework.

Author	Nick Langdon, Director		May, 2018
Date of Next Review			November 2021

Reviewed annually - next date November 2021